LAC

2019冬

セキュリティ診断レポート

特集

セキュリティ診断内製化による脆弱性管理のススメ

セキュリティ診断結果の傾向分析

セキュリティ診断レポート

2019 冬

目次

お客様の手による セキュリティ診断

柳澤 伸幸
セキュリティ診断センター
診断技術グループ　グループマネージャー
2002年よりセキュリティ診断を中心としたコンサルティング業務に従事。
脆弱性診断と緊急対応の知見を活かし、お客様のセキュリティ対策推進を幅広く支援。
2019年から診断センター診断技術グループ グループマネージャーを務める。

「対処」ではなく「確認」を目的とした診断へ

1995年に開始したラックのセキュリティ診断サービスは、インターネットに関する技術革新やお客様のビジネスモデルの変革など、多くの変化に柔軟に対応できるよう、常に進化し続けてきました。その結果、サービス開始当初から続けているサーバやWebアプリケーションを対象としたセキュリティ診断サービスに加え、現在ではスマートデバイスやIoT機器やプロダクト、そして、標的型攻撃といったさまざまな脅威に対する診断サービスも提供できるようになりました。

この間、お客様によるセキュリティ診断の利用方法も大きく変化しました。診断サービスを開始した当初は、脆弱性自体の認知度が低く、セキュリティを考慮した開発手法について情報がなかったため、まずはシステムを作り、その後の診断で見つかった脆弱性を直すという「対処」目的でサービスを利用するケースがほとんどでした。

しかし近年、セキュリティを考慮した開発手法が広く浸透し、従来の「対処」目的のセキュリティ診断から、適切に開発されていることを「確認」する目的のセキュリティ診断に変化しました。このことはサーバやWebアプリケーションを対象とした診断の結果にも表れており、対策が必要となる重要な脆弱性の検出率は年々減少しています。対策におけるミスも少なく、より安全なシステム開発に向かってお客様も確実にスキルアップしています。

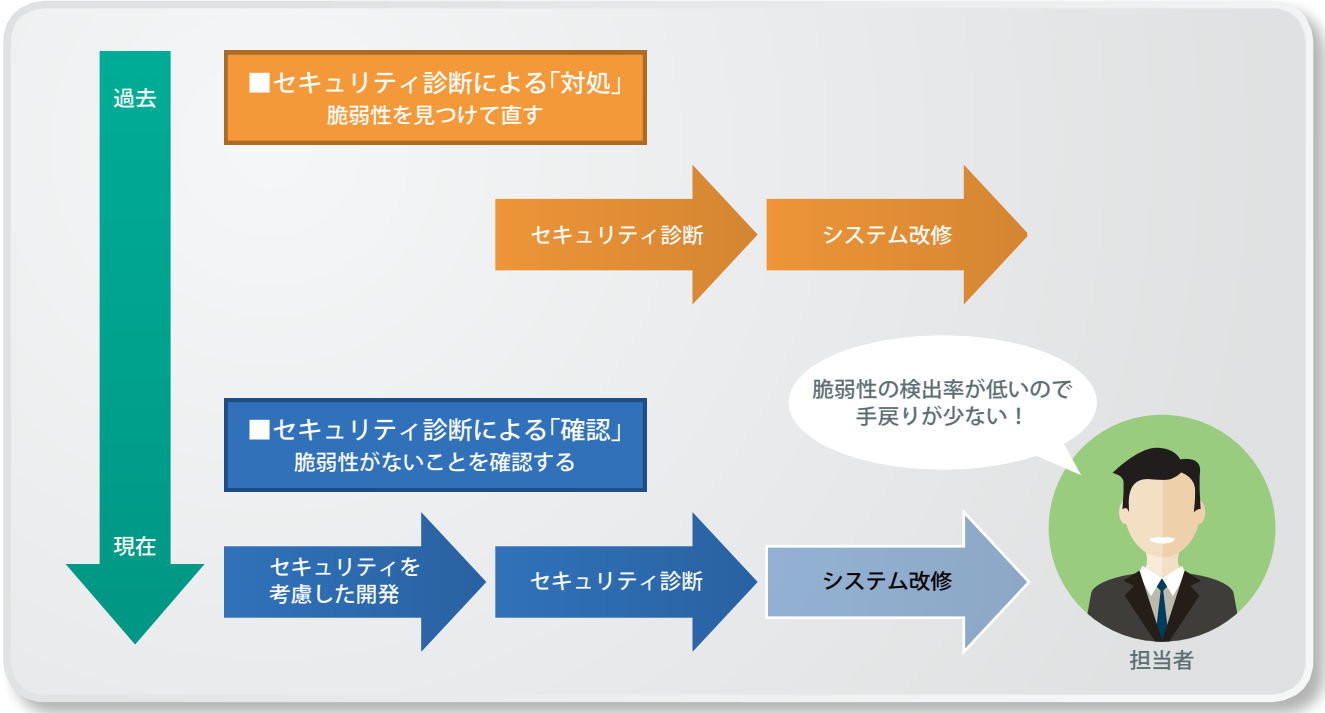
注目を浴びる内製診断

さらに最近になって、従来はセキュリティベンダに依頼していた診断をお客様自身で実施する、「内製診断」の需要が増え始めています。セキュリティ診断を内製化したお客様は、診断期間や対象の調整が柔軟にできるため、リリース後に変更が見込まれるシステムや、アジャイル開発で作るシステムなどに対して診断しやすくなります。

また、内製診断に必要な「脆弱性を確認できる技術」は「脆弱性を作らない技術」とも関係しているため、開発者自身が診断の知識やスキルを身に付けることによって、より安全で堅牢なシステムを開発することにもつながります。

今回のレポートでは、内製診断を利用して脆弱性管理を効率的に行う方法を紹介しています。内製診断を進めるためのステップをできるだけ丁寧にご説明した上で、具体的な事例も記載していますので、お客様ご自身の会社や団体内でのセキュリティ診断を内製化する際の手引きとしてご活用ください。

ネットを通じたサービスがますます多様化して広がる中、セキュリティ対策はますます重要度を増しています。ラックのセキュリティ診断サービスは、お客様やインターネットの安全に貢献するという「思い」や「心構え」を大切に、今後も世の中の変化に併せ進化し続けます。本レポートをお手に取っていただいた皆さまのために、少しでもお力になれれば幸いです。



セキュリティ診断内製化による脆弱性管理のススメ

久原 和起
セキュリティ診断センター
サービスマネジメントグループ
グループリーダー
2006年ラック入社後、開発、診断、顧客診断業務の支援、新サービスの企画等の業務に従事。2018年からグループリーダーを務め、提案活動や導入支援、コンサルティングを行う。

秋田 裕介
セキュリティ診断センター
サービスマネジメントグループ
2002年ラック入社後、セキュリティ監視センターJSOCで監視サービス業務に従事。多岐にわたるセキュリティ製品の導入・運用・保守を経て、現在はセキュリティ診断ツールを中心とした提案活動、導入支援を行う。

昨今は、脆弱性を調査する手段として、内製で実施するセキュリティ診断（以下、内製診断）が注目を浴びています。内製診断は、システム数が多く、開発を頻繁に行っている組織にとってはメリットの大きい診断方法です。本稿では、内製診断を活用して、脆弱性の対応と管理（以下、脆弱性管理）を効果的に行う方法をご紹介します。

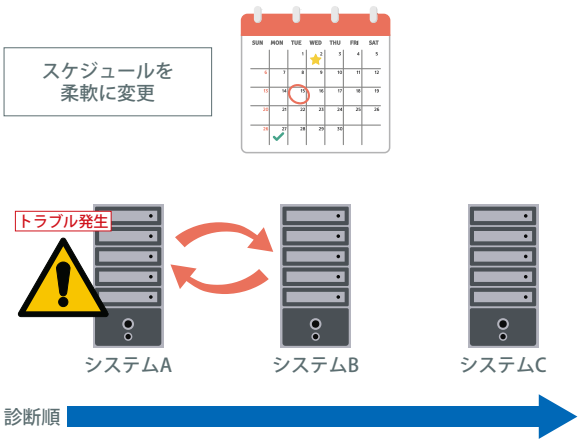
内製診断で円滑な脆弱性管理

昨今のWebビジネスでは、変化し続けるニーズに適応するため短期間に開発・公開を繰り返す開発手法が用いられるようになりました。従来利用されていた外部ベンダによるセキュリティ診断（以降、外部委託診断）では、繁忙期や契約手続等によって、必要なときにすぐに診断できない課題があります。内製診断は自組織内でリソースを調整できるため、開発遅延などによる急なスケジュール変更にも臨機応変に対応しやすくなります。さらに、脆弱性評価基準の統一やコストパフォーマンスのよい診断も可能です。

専門の診断員による外部委託診断は精度が高いですが、内製診断では使用する診断ツールの性能に依存します。しかし、ツールを適切に活用すれば、一定の精度を維持しつつ、外部委託診断より大きなメリットを得られることがあります。以下、内製診断の特徴と効果の詳細をご説明します。

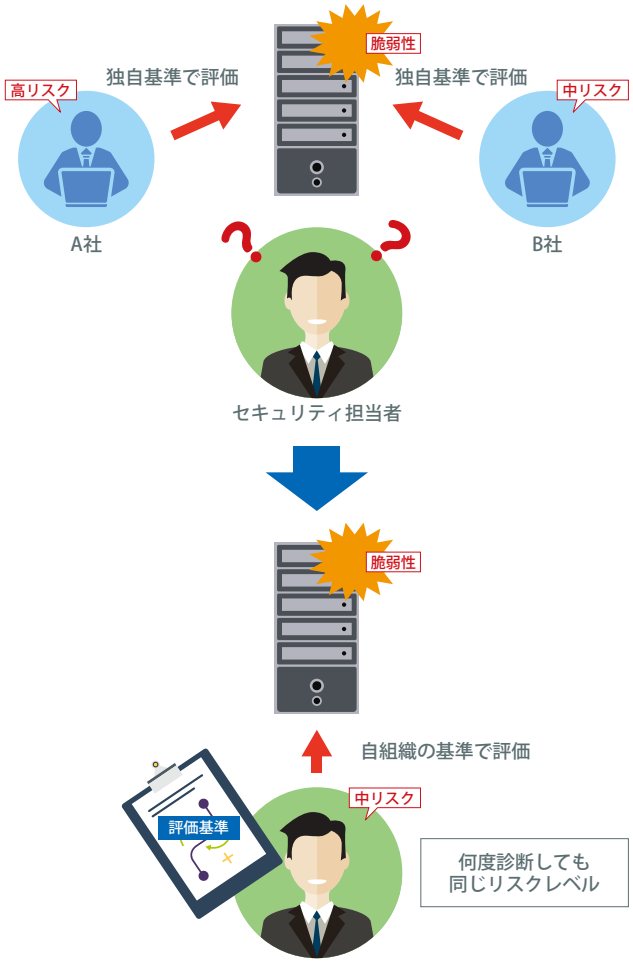
柔軟に診断期間や対象を調整できる

内製診断では、自組織内の関係者と調整するため、診断スケジュールを外部委託診断よりも柔軟に設定できます。突発的なサービス公開やスケジュール変更が発生した場合や、リスクの高い脆弱性情報が公開された場合、自組織内で診断期間や時間帯、対象を組み替えられるため、臨機応変に診断できます。



自組織にとって最適な評価ができる

外部委託診断ではセキュリティベンダ独自の基準で評価されるため、同じ脆弱性であっても委託するベンダによって評価が異なる場合があります。内製診断では、侵入検知・遮断システムといったシステム環境や、攻撃コードの有無による攻撃のしやすさといった点を考慮した脆弱性の一定の評価基準を利用するため、自組織にとって最適な評価を期待できます。



内製診断から脆弱性管理までの4ステップ

診断を内製し、脆弱性管理をするまでの４つのステップを紹介します。
全ての内容を実施することが理想的ですが、実施しながら検討・調整する事項が多いため、
できる範囲から運用を開始し、実践で得た知見や成果をもとに対象範囲を拡大していくことがスムーズな導入のポイントです。

Step1 計画　内製診断を成功に導く土台作り

内製診断では自組織に合った目的や無理のない体制を検討する必要があります。このステップでの主要なポイントは以下の通りです。

●診断目的の検討

自組織のビジネス規模やセキュリティ方針、保有する情報等によって診断目的は変わります。まず、個人情報や企業ブランドなど、守るべきものを決め、インターネットからの不正アクセス、内部不正利用による情報漏えいなど、どのような脅威を想定して診断するかを整理します。そして、目標とするセキュリティレベルや診断範囲、診断内容を決定します。診断範囲には、公開システム、内部システムなどがあります。診断内容には、Webアプリケーション診断やプラットフォーム診断などがあります。

●体制の検討

自組織の状況に合わせて診断を実施する体制を決定します。例えば、診断スケジュールの策定や診断実施はセキュリティ担当者が行い、脆弱性への対応は開発・運用担当者が行うなど役割と責任範囲を定めます。診断担当者が診断を経験したことがない場合は、脆弱性や診断に関する講習・トレーニングを受講しましょう。

また、大規模なシステムの新規公開や定期的な改修などの情報をもとに、システムの重要度に応じた年間スケジュールを策定することで、診断が重なるときに体制を増強できるよう事前にリソース計画を立てます。

●対象システムの選定と診断タイミングの検討

診断目的に基づき、システムの重要度や想定される脅威などを考慮しながら対象システムを選定します。システムの重要度は公開先や用途、利用期間や保有情報などを基に決めましょう。

次に、診断するタイミングを決めます。例えば、システムの新規公開や改修時、定期的な診断、新たな脅威や脆弱性が見つかった時に診断するなどの選択肢があります。

●脆弱性への対応方針を定義

システムの重要度や検出された脆弱性のリスクレベル等を踏まえ、対応期限を含めた方針を定義します。例えば、重要度の高いシステムでリスクレベル「高」の脆弱性が検出した場合は、「即時対応or公開停止」などのルールを定めます。

例　**システム重要度と脆弱性リスクレベルに応じた対応方針**

	脆弱性リスクレベル 高	脆弱性リスクレベル 中	脆弱性リスクレベル 低
システム重要度 高	即時	1週間	1カ月
システム重要度 中	1週間	1カ月	システム部門にて対応期限を設定
システム重要度 低	1カ月	システム部門にて対応期限を設定	システム部門にて対応期限を設定

●内製診断ツールの検討

診断ツールにはさまざまな種類があります。操作のしやすさや診断結果レポートのわかりやすさ、ライセンス形態などを比較し、自組織の目的に合わせたツールを選定します。これまではサポートが充実している商用ツールを導入するケースが主流でしたが、最近はオープンソースの診断ツール(※a) を利用するケースもあります。

●コストの算出

診断ツールの導入や実施にかかる費用、人的コストなどを算出し、コスト計画を作成します。

外部委託診断と併用する場合、外部委託診断と内製診断との割合やそれにかかるコストを検討します。

※a　**オープンソースの診断ツール**：オープンソースの診断ツールの場合、ツールの保守が無い場合がある。また、個人利用以外ではライセンス料などが発生する場合があるため規約やサポート内容の詳細な確認が不可欠。

Step2 診断　担当者が連携してスムーズに診断

Step1で検討した事項に基づき診断を実施します。このステップでの主要なポイントを確認しておきましょう。

●診断前

本番環境と開発環境のどちらを診断するか検討します。正確な結果を得るためには本番環境の診断が理想ですが、診断時にシステム停止など業務影響が発生する可能性があります。業務影響が許容できない場合は開発環境を選択します。万が一に備えてシステムのバックアップを取りましょう。次に、開発・運用担当者に対して、診断日時、診断種別、連絡体制等を伝えます。想定される業務への影響を説明した上で、緊急時には迅速かつ確実に連絡が取れる体制を整備しましょう。必要に応じてクラウド事業者の許可(※b)を得て、監視業者に監視の一時的な停止を依頼することも必要です。

●診断中

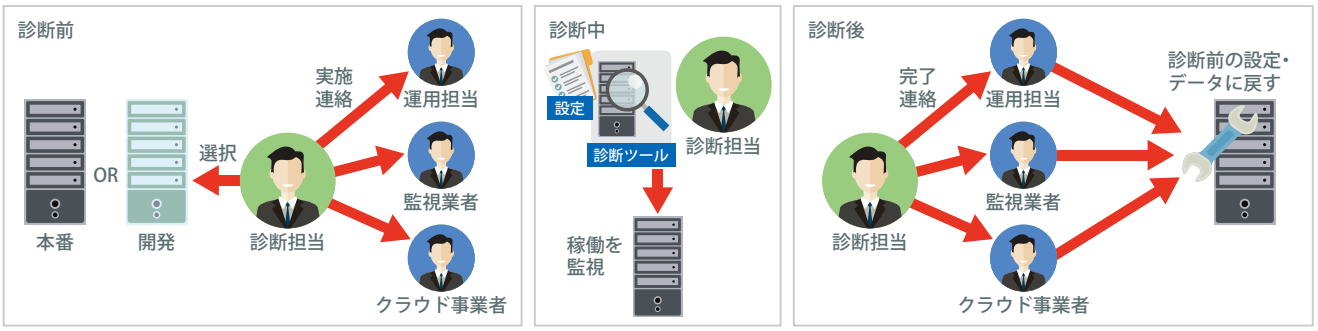
システム障害等のインシデント(※c)につながる可能性があるため、対象外のIPアドレスやドメインなどに診断通信を送信しないよう範囲設定はよく確認して実施します。

問題発生時に即座に対応できるよう診断開始から終了まで、システムの稼働を監視します。万が一、システム障害が発生した場合は、診断停止、関係者への連絡、システム復旧を行い、診断が継続できるようにします。

●診断終了後

診断が終了次第、関係者に診断終了を連絡します。

診断結果に機密情報の漏えいや不正ログインの可能性等、致命的な脆弱性が確認できた場合は、早急に関係各所へ連絡し、サイトの公開停止など緊急対応を行います。また、システムを診断前の状態に戻します。



Step3 対応　確実な対応で脆弱性をなくす

ここでは、検出した脆弱性への対応・管理を行います。以下のようなポイントに留意しましょう。

●対応方法の決定

Step1の対応方針に沿って、システムの重要度や脆弱性のリスクレベルに応じた対応期限を確認します。次に、システム環境や構成、業務影響を考慮して対応方法(※d)を検討します。例えば、セキュリティ製品で検知・遮断できる脆弱性については、暫定的にリスクを回避できるため、次回のシステム改修時に対応する等、具体的な対応時期を明確にしていきます。

●対策の実施

脆弱性ごとに決めた対応方法に従い、対策を実施します。

なお、自組織が管理している他のシステムにおいて、今回検出された脆弱性と同様のものが存在しないか、確認・修正しておくとよいでしょう。

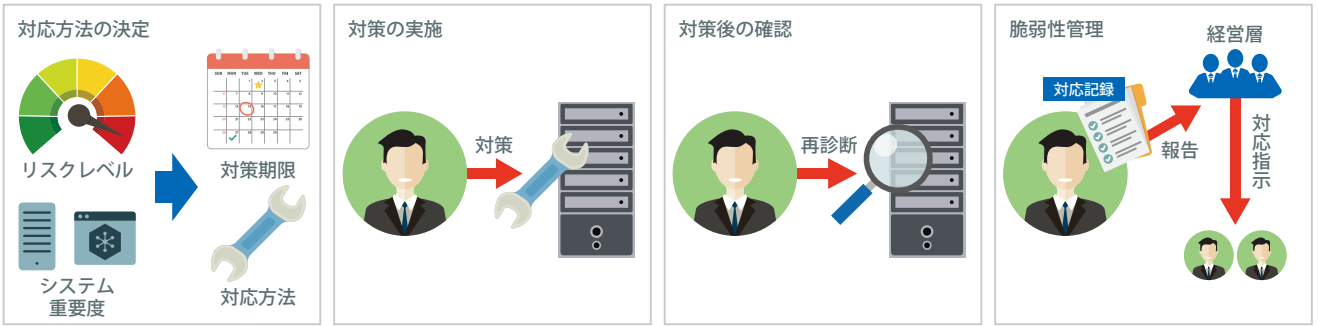
●対策後の確認

定められた期間内に対策が適切に実施されたか確認します。対策漏れや対策が不十分である可能性を考慮し、診断ツールによる再診断を実施し、該当の脆弱性が再び検出されないことを確認します。

●脆弱性管理

対象システムで検出した脆弱性ごとに対応記録(※e)を残します。対応記録に基づき、次回改修時に対応予定の脆弱性や、代替策しか実施しておらず根本的に解決していない脆弱性は、引き続き対応状況(※f)を確認しましょう。

全社的な脆弱性対応状況は定期的に経営層と連携し、対応できていない部署に対してトップダウンで指示するとよいでしょう。



※b　**クラウド事業者の許可**：診断通信が本物の攻撃と誤認されることがあるため、クラウドサービスの提供業者によっては、診断の事前申請が必須な場合がある。
※c　**インシデント**：事業運営を危うくする確率及び情報セキュリティを脅かす確率が高い事態。
※d　**対応方法**：検出された脆弱性の中には、誤検出が含まれていることがある。誤検出が疑われる場合には、設定やパッチ、Webアプリケーションの実装の状態を確認する。
※e　**対応記録**：対応有無、対応完了日、代替策の実施有無等、自組織内で脆弱性管理に必要な情報を記録する。
※f　**対応状況**：残存している脆弱性で新たな攻撃手法が発見された場合、緊急的に対応が必要なケースがある。脆弱性のリスクレベルに変化がないか適宜確認することを推奨する。

Step4 改善　開発から脆弱性管理までの方法を見直し

開発から脆弱性管理まですべての工程を改善します。このステップでの主要なポイントは以下の通りです。

●内製診断のレベルアップ

診断ツールで検出した脆弱性を担当者が詳細に調べることで、攻撃手法や対策への理解が深まります。

それにより、攻撃者の視点に立ったチェックを行う手動診断の技術習得につながり、診断ツールによる機械的なチェックでは見つかりづらい脆弱性を検出できるようになります。診断ツールによる診断が安定的に運用できるようになったら、次のステップとして手動診断を取り入れた詳細な診断を行い、全社的にセキュリティレベルを向上させましょう。

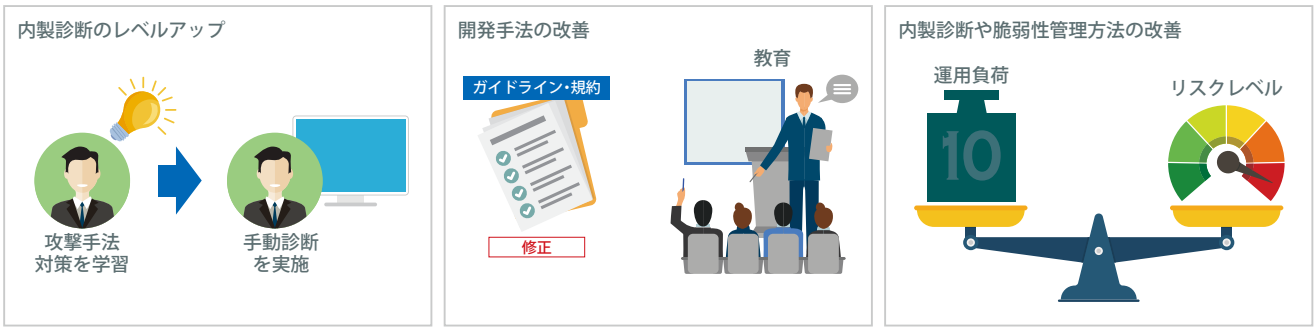
●開発手法の改善

自組織でよく検出される脆弱性については、脆弱性を再発させないため、設計のガイドラインやコーディング規約を修正します。Webアプリケーションであれば IPA発行の「安全なウェブサイトの作り方」(※g) やOWASP発行の「OWASP Top 10 Proactive Controls」(※h) を参考にするとよいでしょう。また、開発者にセキュリティを考慮した開発手法を教育し、開発工程の早い段階で脆弱性のある作り込みを予防しましょう。

●内製診断や脆弱性管理方法の改善

内製診断や脆弱性管理の方法は適宜見直しましょう。

運用を継続していると、組織体制やセキュリティ方針の変更等により、ルールや運用方法が組織の実態に合わなくなることがあります。セキュリティレベルを上げるためにルールを厳しくしていくだけではなく、脆弱性対応による運用負荷とリスクレベルを天秤にかけ、バランスのよいルールとなるよう見直します。



事例の紹介

内製診断による脆弱性管理の事例を紹介します。

Case 1　できる範囲から内製診断を始める

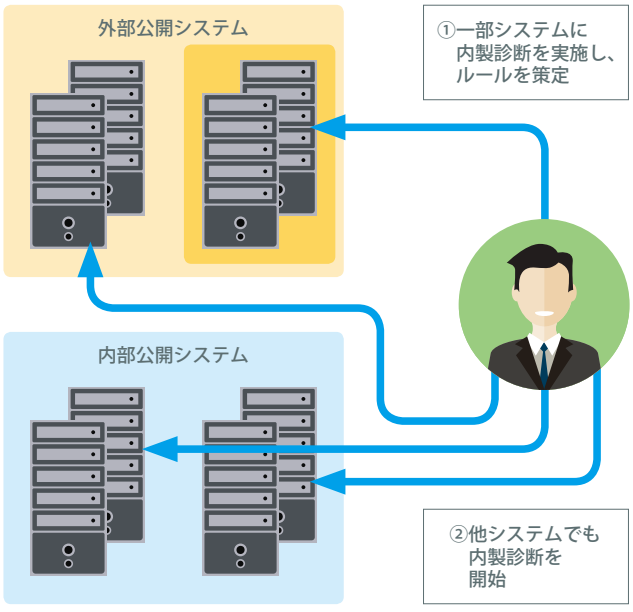
ルールがなく、運用方法が部署ごとにバラバラであったお客様が内製診断を取り入れた事例です。

このお客様は、システムをインターネットへ公開する前段階で部署ごとに外部委託診断を利用していましたが、対象システムの選定や脆弱性の対応基準、時期等の決定を都度独自に実施しており、統一したルールがありませんでした。そこでセキュリティレベル底上げのため、セキュリティ担当が全組織内を同じ基準で評価できる内製診断の導入を検討しました。

内製診断のルール策定のため、まずは一部のシステムを対象として取り組みを開始しました。対象システムを絞ったことにより、開発・運用担当者と十分なコミュニケーションをとることができ、協力を得ながら自組織に適したルールや運用方法、体制を決めることができました。

次に、インターネット公開システム全てを対象に内製診断を始めました。すでに実績や効果が見えていたため、経営層の承認も得やすく、スムーズに展開することができました。手順や運用方法の一部を修正し、各部門のシステムに対して内製診断を実施できるようにしました。

その後、内部システムにも範囲を拡大し、定期的にルールを見直しながらセキュリティ強化に努めています。

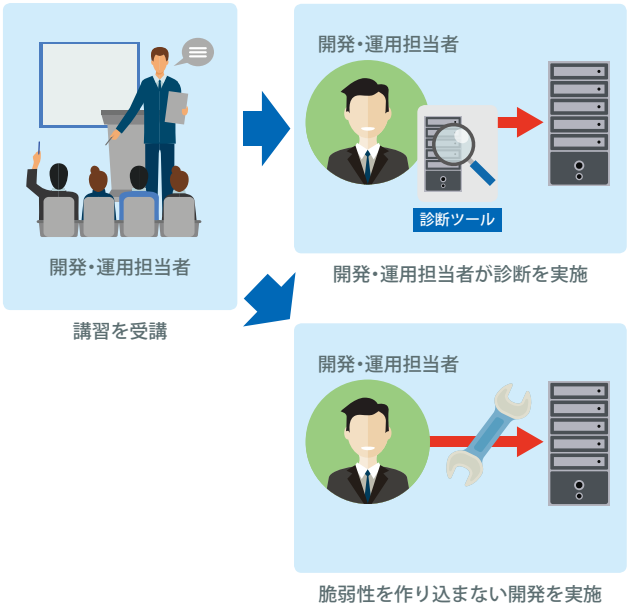


※g　独立行政法人 情報処理推進機構(IPA)「安全なウェブサイトの作り方」：https://www.ipa.go.jp/security/vuln/websecurity.html
※h　Open Web Application Security Project (OWASP)「OWASP Top 10 Proactive Controls」(日本語訳)：https://www.owasp.org/images/a/a8/OWASPTop10ProactiveControls2016-Japanese.pdf

Case2　開発・運用担当が内製診断を実施

開発・運用担当者が中心となり内製診断を実施した事例をご紹介します。

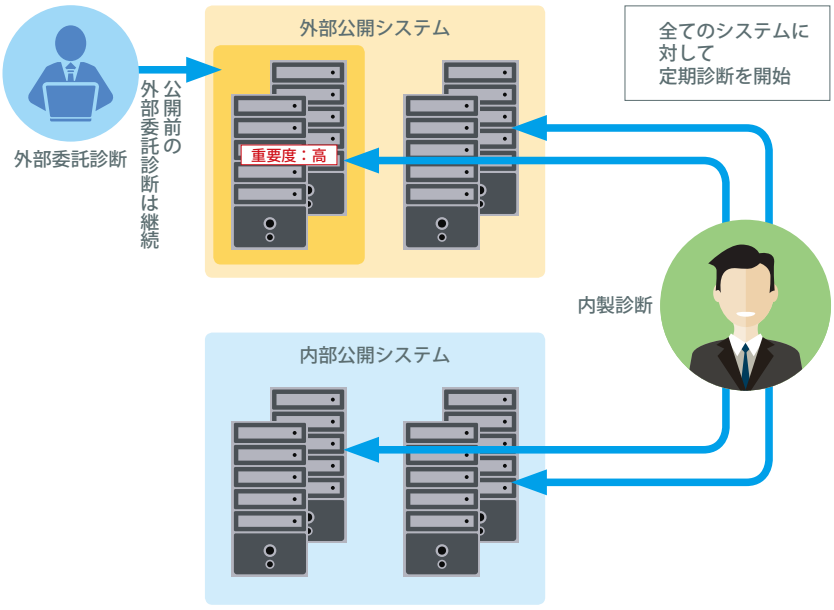
　このお客様は、顧客ニーズや世間の動向に合わせて新規サービス公開や既存サービスに対する機能追加を頻繁に実施していました。
　もともと開発・運用担当者によるセキュリティを含めたIT全般に対する関心が高い状態であったため、開発・運用担当者が診断ツールのトレーニングや、診断方法及び脆弱性の考え方に関する講習を受講することにより、自ら内製診断を実施できるようになりました。加えて、運用が安定するまでは、ラックの専門家がお客様先に定期訪問し、内製診断の実業務において、診断ツールの具体的な設定方法やトラブルシューティング等の支援をしました。
　このお客様では、開発工程のテストフェーズの一環として脆弱性診断を追加しました。診断後、開発者自らが対応できるため、対策にかかる期間を短縮することができました。
　また、開発者自身がセキュリティスキルを身に付けることで、脆弱性を作りこまない開発手法を主体的に実施する意識が生まれ、セキュリティを考慮した開発標準が浸透しました。公開前に実施する脆弱性診断だけを頼るのではなく、構築・開発のより早い段階で脆弱性対策を行う開発プロセスが定着しています。



Case3　外部委託診断と内製診断を併用

システムの重要度に応じて外部委託診断と内製診断を併用する方法を採択したお客様の事例です。

　このケースでは、重要度の高いシステムに対してのみ公開前に外部委託診断を実施していました。しかし、同業他社のセキュリティ事故事例を受け、全体的なセキュリティレベル向上を目的として重要度の低いシステムも脆弱性診断を実施することになりました。
　コスト面を考慮して、まず全てのシステムに最低限のセキュリティレベルを担保するための内製診断を導入しました。内製診断を定期的に行うことで、システム全体の脆弱性状況を管理・把握できるようになりました。それに加え、新規の脆弱性に対しても迅速な対応ができるようになり、全社的にセキュリティレベルが向上しました。
　また、全てを内製診断には置き換えるのではなく重要度の高いシステムに対する外部委託診断は継続することで、セキュリティレベルとコストのバランスをとった脆弱性管理を実施しています。



おわりに

「内製診断」を利用した脆弱性管理の方法について、事例を交えて解説しました。
　自組織内での内製診断による脆弱性管理には、組織体制の変化や開発プロセスの変更などに応じて、随時見直しながら最適化していくことが重要です。
　弊社の「セキュリティ診断内製化支援サービス」では、経験豊富なスタッフがお客様の環境に最適な方法を提案し、脆弱性診断の全体的なコストを抑えつつ、お客様のセキュリティレベルの向上を支援します。ご検討の際には、お気軽にご相談ください。

セキュリティ診断結果の傾向分析
Webアプリケーション診断 ならびにプラットフォーム診断

花岡 顕助
セキュリティ診断センター　担当部長
2002年ラック入社後、セキュリティ監視センターJSOCで監視サービス業務に従事。
2013年よりWebアプリケーション診断グループにて診断業務を行う。
現在は診断コンサルタントとして大規模なセキュリティ診断案件のリーダーを務める。

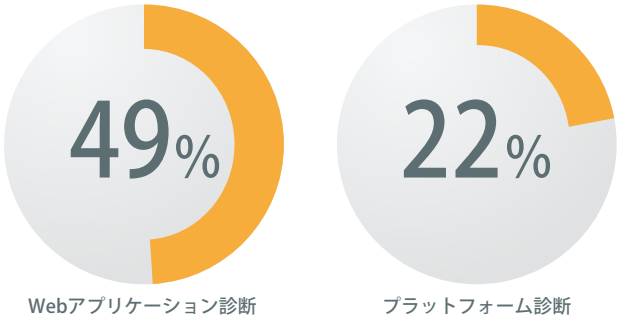
1 5割のWebアプリと、2割のホストにMediumリスク以上の脆弱性あり

2018年に実施したセキュリティ診断結果の傾向を分析したところ、セキュリティ上の重要な脆弱性(High/Mediumリスク)が検出された割合は、Webアプリケーション診断では全サイトの49%、プラットフォーム診断では全ホストの22%に上りました(図1)。

Webアプリケーション診断の検出割合は2017年の54%を下回りましたが、引き続き2サイトに1サイトは何らかの対策が必要な状況にあり、Webアプリケーション開発におけるセキュリティ対策の強化が強く望まれます。

プラットフォーム診断での検出割合は、2017年より9ポイント下がり2014年以降の過去5年で最も低い値となりました。理由は、定期的に診断しているシステムで脆弱性対策が進み検出数が減ったこと、また、セキュリティアップデートが十分に機能し、より新しい脆弱性への対策が適切に行われていることが考えられます。

図1 重要な脆弱性(High/Mediumリスク)を検出した診断対象の割合



2 診断件数の推移

全体を俯瞰するため、2008年以降において診断件数の変化を集計した後、業種やサービス種別など個別の傾向を見るために直近の5年に焦点を絞って分析しました。

●診断件数は10年前の倍以上に

2018年の診断件数は10年前の2008年に比べ、Webアプリケーション診断は4.0倍、プラットフォーム診断は2.5倍になりました(図2)。特にWebアプリケーション診断は、定期診断や新規開発・改修時の診断が増え、ここ数年は前年比で1割程度増加し続けています。その理由としては、Webサイトへの不正アクセスによって情報漏えい事件が多発しセキュリティ診断の必要性が広く認知されたこと、また、自社が保有する公開Webサイトへのセキュリティ診断がお客様のセキュリティポリシーで義務付けられたこと等が挙げられます。これにより同一のお客様から一度に依頼されるサイト数が増加しています。一方、プラットフォーム診断については、ランサムウェアの被害が世界中で発生し、その脅威が世間に認知されるようになった2016年以降、プラットフォーム環境のセキュリティ強化が必要との認識が広まり、診断依頼が増加しました。

●業種別診断件数の割合

業種別に見ると、Webアプリケーション診断は2017年に比べて「金融」「サービス」「製造」の割合が増加しました(図3)。理由は、診断を継続的に利用しているお客様で、新サービスの公開や業務システムの入替に伴う新規のWebサイトに対する診断件数が増加したこと、また、セキュリティポリシーの見直しに伴う現状把握を目的としたWebサイトの一斉診断により新規のお客様が増えたことが考えられます。

プラットフォーム診断については、「官庁・公共」だけで全体の6割を占め、「金融」「情報・通信」の3業種で9割を占めています(図4)。これらの業種では、新規構築したシステムに対する診断に加え、運用中のシステムに対する定期的なセキュリティ診断を実施しています。

図2 診断件数の増加(2008年～2018年)

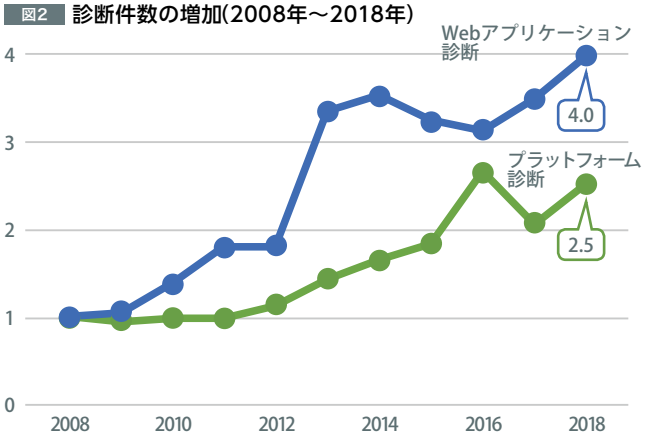


図3 業種別対象Webサイトの割合推移
（Webアプリケーション診断）

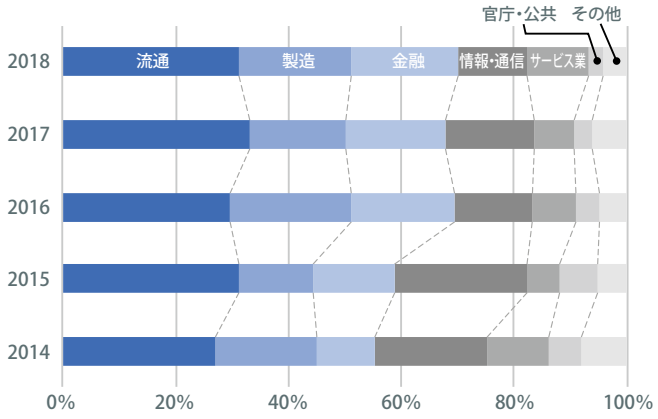
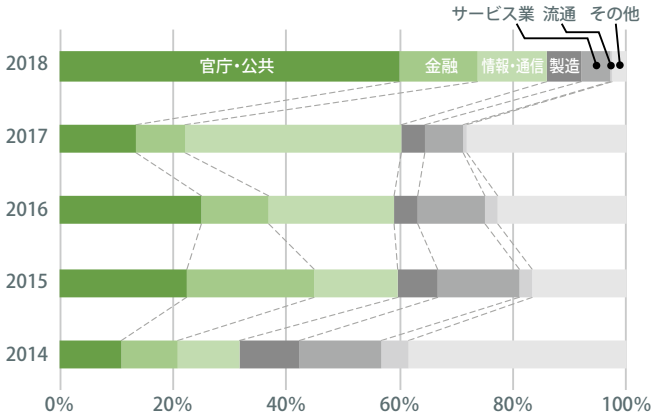


図4 業種別対象ホストの割合推移
（プラットフォーム診断）



3 選択されたサービスの分析

●診断期間と品質のバランスが重視される

各診断でお客様が選択したサービス（図５）の割合を調査しました。2018年も全体の傾向に変化はなく、Webアプリケーション診断は「ハイブリット診断」と「ライト診断」でほぼ100%、プラットフォーム診断は「スタンダード診断」の割合が一番多くなりました（図6・7）。

Webアプリケーション診断には、お客様のニーズに応じて「アドバンスト診断」、「ハイブリッド診断」、「ライト診断」の3種類のメニューを用意しています。

「アドバンスト診断」はすべての入力パラメータに対して手動による疑似攻撃を試行し、隅々まで徹底的に診断します。外部公開するシステムで高度なセキュリティが求められ、また、十分な診断期間が設定できるケースで選ばれる傾向にあります。

「ハイブリッド診断」では、「アドバンスト診断」の約1/4の期間で代表的な疑似攻撃パターンを確認します。さらに短期間で診断を実施したい場合は、2日程度で可能な範囲を診断し、脆弱性の傾向を把握する「ライト診断」が選ばれます。過去5年を通して「ハイブリッド診断」と「ライト診断」でほぼ100%の割合を占めており、依然として、診断期間と網羅性のバランスが求められる現状が伺えます。

プラットフォーム診断には、市販ツールと独自ツール、手動診断を組み合わせて実施する「アドバンスト診断」と、市販ツールと独自ツールにより実施する「スタンダード診断」、市販ツールで実施する「エクスプレス診断」の3つのサービスがあります。

「アドバンスト診断」は、Webアプリケーション診断と同様に高度なセキュリティ対策が求められるお客様にニーズがあるサービスです。具体的には、「金融」「情報・通信」のお客様が、外部公開しているシステムの診断で利用するケースがほとんどです。

「スタンダード診断」は診断期間と精密さのバランスが良いサービスです。幅広い業種のお客様で利用されており、2018年は68%のお客様がこのサービスを選択しています。

「エクスプレス診断」は短期間で診断できるため、大量のホストに対して診断が必要な場合によく選択されるサービスです。

近年は、自組織内で市販ツールを購入し自ら診断する、「内製診断」に関心が集まっています。内製診断を導入するお客様が増えた場合は、市販ツールのみの「エクスプレス診断」ではなく、ラックの知見を活かした「スタンダード診断」や「アドバンスト診断」の選択するお客様が増えると予想されます。

図5 サービスメニュー

Webアプリケーション診断		プラットフォーム診断
サービス	診断目的	サービス
アドバンスト すべての入力パラメータに対して手動で詳細診断	詳細確認	**アドバンスト** 市販ツール、独自ツール、手動によって詳細診断
ハイブリッド ツールと手動の組み合わせ。主要問題点についてサイト内を網羅的に診断		**スタンダード** 市販ツールと独自ツールの組み合わせで診断
ライト ツールと手動でサイト内の主要機能をサンプリングして診断	傾向把握	**エクスプレス** 市販ツールのみで診断

図6 サービス別診断件数の割合（Webアプリケーション診断）

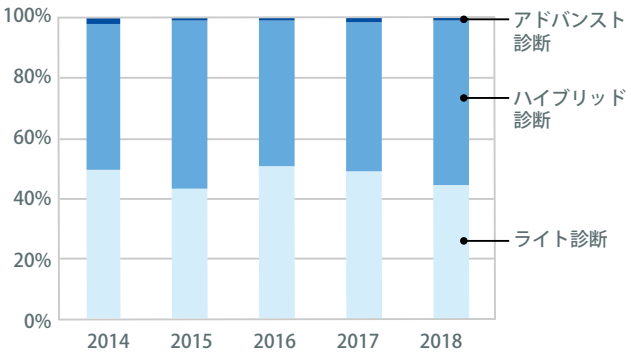
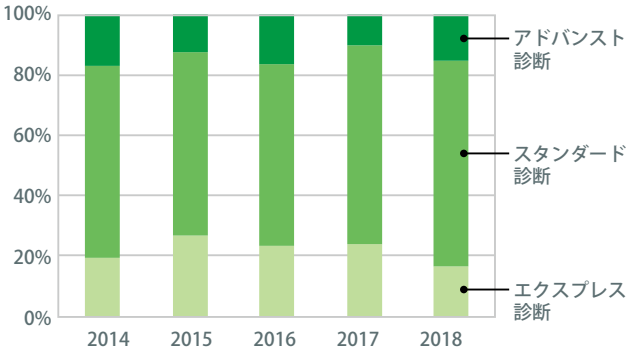


図7 サービス別診断件数の割合（プラットフォーム診断）



●リモート診断が大半を占める

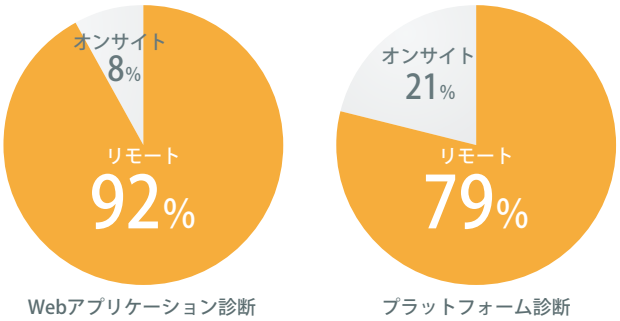
セキュリティ診断の実施方法には、インターネット経由でアクセスするリモート診断と、お客様が指定する場所で実施するオンサイト診断の2通りがあります。

Webアプリケーション診断では例年リモート診断の割合が大半を占め、2018年は92%に上りました(図8)。これは、オンサイト診断に比べて費用と準備作業の負担が少ないため、ラックへのアクセス制限を一時的に解除(※i)した状態でのリモート診断を選ぶお客様が多いことが理由です。

オンサイト診断は、診断対象サイトが外部接続を許可していない環境に存在し、物理的にリモート診断ができない場合に選ばれます。どちらの診断を選んだとしても、ファイアウォールなどによるアクセス制限がない状態でWebアプリケーション単体の診断を行うため、診断項目、結果の品質に差異はありません。

プラットフォーム診断は全体の80%をリモート診断が占めています。定期診断を目的としたケースが多いため、運用の一部にリモート診断が組み込まれていることがわかります。プラットフォーム診断では、外部脅威を想定した診断をする場合は、ファイアウォールなどによるアクセス制限はそのままでリモート診断を実施します。ホスト単体での診断をしたい場合はオンサイト診断を実施します。Webアプリケーション診断とは異なり、同じホストに対する診断でも、実施方法によって違う結果が得られます。

図8　2018年　診断経路の割合



4　検出された脆弱性の分析(Webアプリケーション診断)

●5サイトに1サイトはHighリスクを検出

Webサイトで検出された脆弱性のうち、最もリスクレベルが高いものをそのサイトのリスクとして集計し、割合の推移を図9にまとめました。Webアプリケーション診断では、過去5年を通してすべてのWebサイトで脆弱性を検出しています。

2018年は、重要な脆弱性(High/Mediumリスク)を検出したサイトが、全体の49%を占めました。年々割合は減少していますが、未だに2サイトに1サイトは対策が必要な状況です。最も緊急度の高いHighリスクについては、経年の減少傾向はなく、毎年5サイトに1サイトの割合で検出しています。

脆弱性が作られてしまう主な要因としては、開発プロセスで機能要件を満たすことが優先され、セキュリティ要件が十分に考慮されないことが挙げられます。機能要件とセキュリティ要件の「両立」を意識することが、Webアプリケーションの品質向上につながるという価値観を依頼側と開発側とで共有することは重要です。Webアプリケーションのセキュリティ対策の重要性や方法について、講習や勉強会などを通じて関係者が理解を深めることが効果的な対処方法の一つです(図10)。

図9　リスクレベル別 診断対象Webサイトの割合

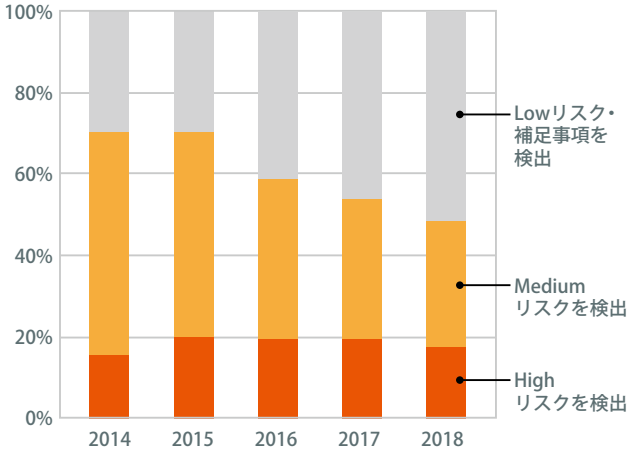
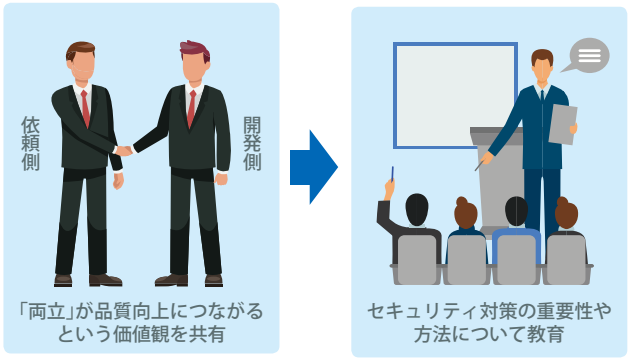


図10　機能要件とセキュリティ要件の両立



●HTTPS化が進むものの対策は不十分な状態

2018年に実施したWebアプリケーション診断で、検出頻度が高かった重要な脆弱性のうち、上位10件を表1に示します。

2018年は、2017年とほぼ同じ脆弱性がランクインしました。Webサイトの HTTPS化が進んだため「HTTPで重要な情報を送信」が3位から5位に下がった一方、HTTPS化で対策必須となる「HTTPSのCookieにsecure属性の指定なし」が2位にランクインしているため、対策が不十分な傾向が見られました。

表1　2018年に検出した重要な脆弱性　上位10件

順位	脆弱性名		検出割合
1位	クロスサイトスクリプティング	➡	16.0%
2位	HTTPSのCookieにsecure属性の指定なし	➡	14.7%
3位	クロスサイトリクエストフォージェリ	⬆昨年4位	12.1%
4位	データ識別子改ざんによるシステム不正利用(機微な情報の露出)	⬆昨年5位	9.8%
5位	HTTPで重要な情報を送信	⬇⬇昨年3位	8.8%
6位	権限昇格が可能(機微な情報の露出)	➡	7.1%
7位	SQLインジェクション	⬆昨年8位	6.8%
8位	URLに重要な情報を格納	⬇昨年7位	6.5%
9位	診断時の送信データによるシステム停止	➡	1.9%
10位	強制ブラウジング	⬆昨年12位	1.4%

※i　**一時的に解除**：ファイアウォール等においてラックの外部IPアドレスを一時的にアクセス許可リストに加える、また、発行されたクライアント証明書を使ってVPN接続をするなどしてWebアプリケーションにアクセスする。

●対策が標準化できない脆弱性の検出割合は横ばいで推移

上位10件の脆弱性を「①対策が標準化できる脆弱性」と「②対策が標準化できない脆弱性」に分類し、過去5年の検出割合を調査しました(図11)。

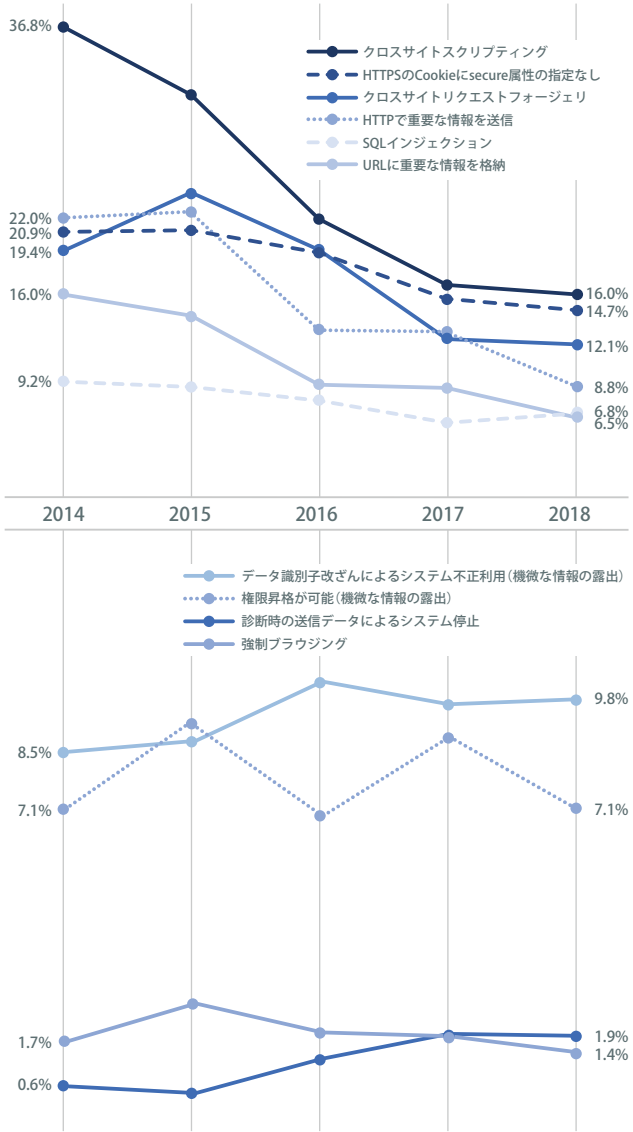
①対策が標準化できる脆弱性……脆弱性ごとに一律に対策可能な脆弱性
②対策が標準化できない脆弱性……構成や機能を考慮して、システムごとに対策を検討する必要がある脆弱性

①の脆弱性は年々検出割合が減少していますが、②の脆弱性はほぼ横ばいの状態であることがわかりました。

①の脆弱性は、情報漏えい事件などにより危険性が世間的に認知されているものが多く、また、対策が標準化されていることによりセキュアな実装方法を普及しやすい状態です。そのため、ここ数年で開発現場におけるセキュアプログラミングの浸透がさらに進み、脆弱性の検出割合が減ったと考えられます。①の対策は一部の開発言語やフレームワークの仕様にも取り込まれ、設計段階でセキュリティ要件が十分に検討されていない場合でも、脆弱性が作りこまれにくい環境が整ってきています。

②に分類されている脆弱性はいずれもリスクレベルの高いものですが、①に比べてあまり対策が進んでいません。その背景には、構成や機能を考慮して、システムごとに対策を検討する必要があり、対策漏れが発生しやすいことがあります。また、①と違って開発言語などの仕様に対策が取り込みづらいため、セキュリティ要件の検討が不十分な場合は脆弱性が作り込まれてしまいます。

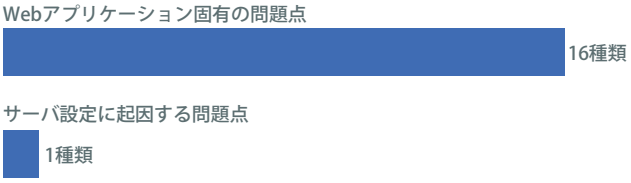
図11 脆弱性の検出割合の推移



●Highリスクが検出される要因

2018年には、最も緊急度の高いHighリスクの脆弱性を17種類検出しました。そのうち16種類がシステム開発時の設計・実装に起因するWebアプリケーション固有の問題点であり、残り1種類はWebサーバ設定に関する問題点でした(図12)。特に、Webアプリケーション固有の問題点を検出したケースでは、大きく二つの特徴が見られました。一つは①脆弱性のあるコードの使いまわし、もう一つは②パッケージ製品の使用です。

図12 2018年に検出したHighリスク問題点の種類



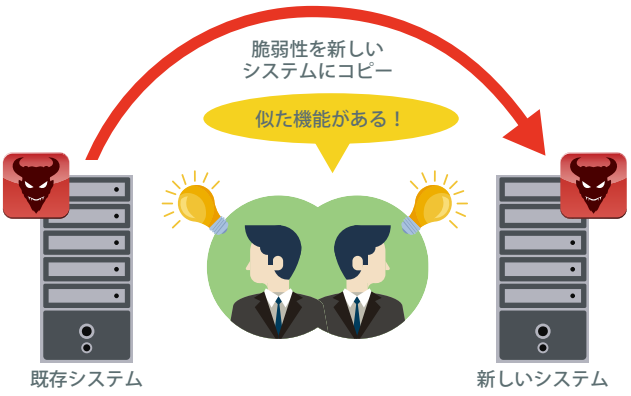
①脆弱性のあるコードを流用したシステム

システム構築の際に、類似機能のあるWebアプリケーションからコードを一部流用したことにより、流用元に含まれる脆弱性も同時にコピーされてしまったケースです(図13)。

脆弱性のあるコードを流用したシステムでは、重要度の高い脆弱性を複数種類検出する他、「Low」「補足事項※j」の脆弱性を10種類以上検出することが多くあります 。この要因としては、流用元のWebアプリケーション診断では、セキュリティを考慮した開発手法が開発時には普及していなかったことや、これまでセキュリティ診断を実施したことがなかったことなどが考えられます。

Webアプリケーションがセキュリティ対策を考慮せずに構築されていた場合、さまざまな面で問題が存在する可能性があります。ラックが確認した中には、時間短縮のために、脆弱性があるとは知らずにコードを流用したケースがありました。安易に他システムからコードを流用することは避け、システム全体でセキュリティ対策が行われている状態にしましょう。なお、コードを流用せざるを得ない場合は、セキュリティチェックを適切に行い、脆弱性を取り除くことが必要です。

図13 脆弱性のあるコードを流用



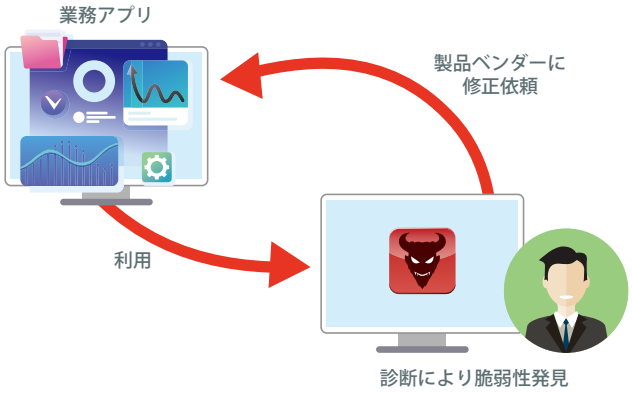
※j　**補足事項**：Webアプリケーション診断では、軽微な脆弱性は「補足事項」として報告している。

②パッケージ製品で構築されたシステム

基幹業務用のパッケージ製品を導入したシステムで、Highリスクの脆弱性が検出されるケースも複数ありました。

パッケージ製品を用いたシステムでは、利用者が設定変更した箇所に脆弱性が検出されることが多い傾向にありますが、2018年は、ログイン画面などの製品の基本機能部分に脆弱性が検出されることが複数ありました。このような場合、対策は製品ベンダに問題点の修正を依頼することになります。パッケージ製品を選定する際は、ベンダ側でのセキュリティ診断の実施状況を確認し、導入後に脆弱性が発見された場合の対応を保守契約に含めるなどの対応が重要です(図14)。ベンダによる問題点修正が長期にわたる場合は、システム全体に多段防御の仕組みを取り入れることで脆弱性による影響を最小限に留めることが可能です。

図14 パッケージ製品の基本機能部分における脆弱性対応



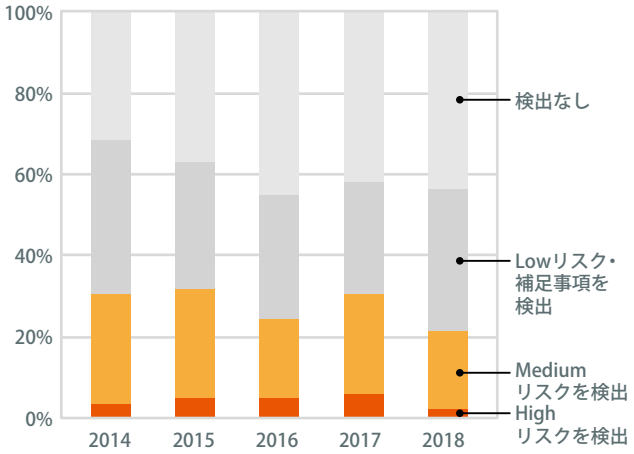
5 検出された脆弱性の分析(プラットフォーム診断)

●5台に1台はOS・ミドルウェアの対策が必要

プラットフォーム診断で検出された脆弱性のうち、最もリスクレベルが高いものをそのホストのリスクとして集計し、割合の推移を図15にまとめました。2014年から2017年までは、重要な脆弱性(High/Mediumリスク)が検出されたホストの割合は30%前後で推移していましたが、2018年は、リモート診断、オンサイト診断ともに検出率が下がり、22%と過去5年間で最も低くなりました。これは、プラットフォーム診断を活用した組織において、パッチの適用やアクセス制限等の対策が実施された結果と考えます。

また、2018年はHighリスクの検出割合が顕著に減少しています。特にOS認証を突破できる件数が少なくなっているため、アカウント管理に関する規定を設け、適切に運用している組織が増加しつつあると考えられます。重要な脆弱性の検出数は減少傾向にありますが、依然として5台に1台はOS・ミドルウェア(OSとアプリケーションの中間で働くプログラム)の対策が必要な状況であり、引き続き注意が必要です。

図15 リスクレベル別 診断対象ホストの割合

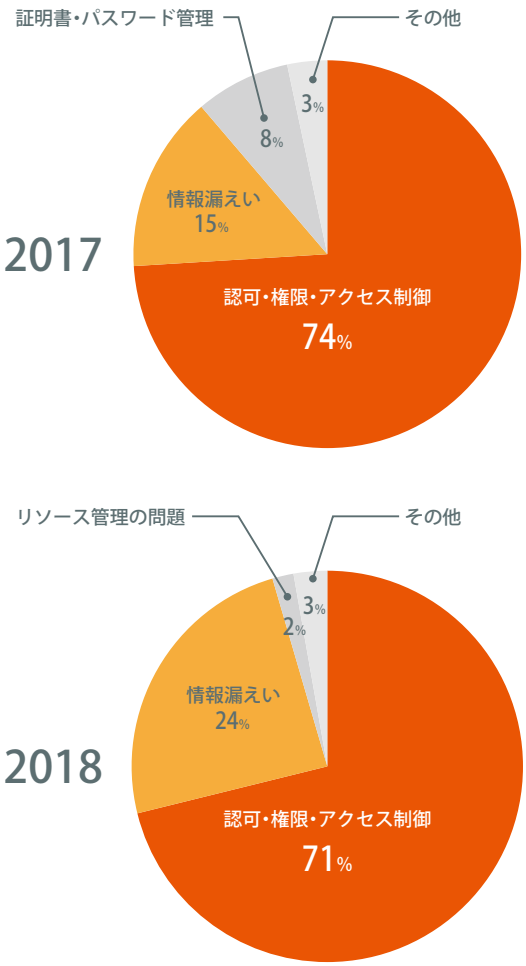


●「情報漏えい」に分類される脆弱性の割合が増加

脆弱性の傾向を分析するため、共通脆弱性タイプ一覧CWE(※i)を使って、脆弱性の種別を調査しました。調査対象は、検出された重要な脆弱性の上位20件です(図16)。その結果、「許可・権限・アクセス制御」と「情報漏えい」に分類される脆弱性は2017年の89%から2018年は95%となりさらに大きな割合を占める結果となっています。

参考として「許可・権限・アクセス制御」「情報漏えい」に分類される代表的な脆弱性を(図17)に記載します。

図16 2017年と2018年に検出された脆弱性の種別

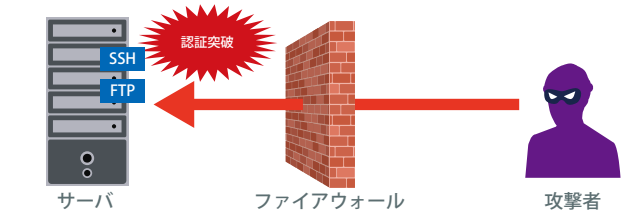


2018年は2017年に比べて「情報漏えい」の割合が約10ポイント増加しています。これは、「情報漏えい」に分類される脆弱性が新たに発見されたことが一因だと考えられます。例えば、2018年8月には「OpenSSH にユーザ名列挙の脆弱性(CVE-2018-15473※

※k 共通脆弱性タイプ一覧CWE:米国政府の支援を受けた非営利団体のMITREが中心となり仕様策定をした、脆弱性の種別を識別するための世界的な共通基準。Common Weakness Enumerationの略。
※l CVE-2018-15473:https://nvd.nist.gov/vuln/detail/CVE-2018-15473

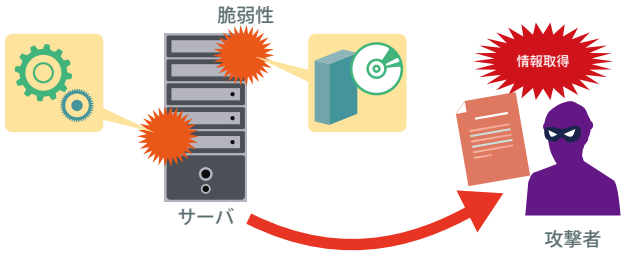
l)」が公開されています。この脆弱性は、攻撃者が特別に細工したパケットをサーバに送信した場合に、応答内容の違いを利用してサーバに存在するアカウント名を取得する脆弱性です。2018年のプラットフォーム診断では、約1割のホストで検出しました。このように、OSやミドルウェアでは新たな脆弱性が日々発見されるため、過去の診断で問題がなかったホストでも新しい脆弱性が検出される場合があります。セキュリティレベルを維持するためには、OSやミドルウェアのアップデートを定期的に行い、それらの対策が適切に実施されていることを継続して確認することが重要です。

図17 代表的な脆弱性



(例)パスワード認証を施行可能

ファイアウォール等でIPアドレスによるアクセス制限が施されておらず、パスワードクラックによって認証を突破される可能性がある



(例)情報取得が可能

ソフトウェアのバージョンが古かったり、設定に不備があったりすることが原因で、ホストのアカウント名などシステム情報が取得できる

●市販の脆弱性スキャナでは見逃しがちな脆弱性

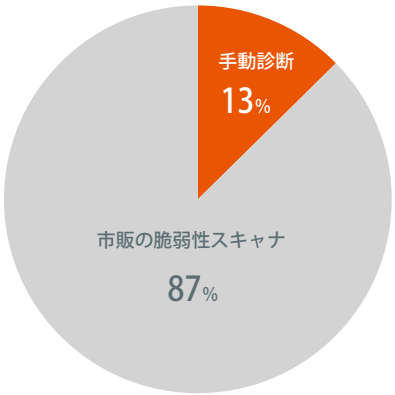
昨今のプラットフォーム診断では、市販の脆弱性スキャナ(以下、スキャナ)の診断精度が向上したため、多くの脆弱性を検出できるようになりました。しかし、スキャナのみでは検出困難な脆弱性もまだ多く存在します。2018年に検出された重要な脆弱性のうち、スキャナで検出できる脆弱性と手動診断でなければ検出できない脆弱性の割合を図18にまとめました。スキャナが適切に実行できた場合は9割近くの脆弱性を検出できますが、1割は手動診断でなければ検出できません。手動診断でなければ検出できない脆弱性のなかには、重要度の高い脆弱性が含まれる場合もあります。

手動診断でなければ検出できない脆弱性には、システム情報や重要情報が不用意に表示されたWebページの検出などがあります。スキャナはWebページに表示された情報の重要度を判断できないため、脆弱性として検出しません。

また、複数の脆弱性を組み合わせることによって検出が可能になる脆弱性は、スキャナを実行しただけでは発見できません。例えば、アカウント情報が取得できる脆弱性と、管理コンソールにおいてパスワード認証が有効である脆弱性を利用して、システムにログインできる場合がありますが、スキャナでは見逃されます。

スキャナで検出困難な脆弱性を検出するために有効なのが、専門家による手動診断です。手動診断では、スキャナが持つ特性を把握し、十分に診断できない箇所を重点的に診断します。特に、攻撃された場合の影響が大きいシステムについては、スキャナと手動診断を併用した診断サービスを選ぶ必要があります。

図18 市販の脆弱性スキャナと手動診断で検出された脆弱性の割合



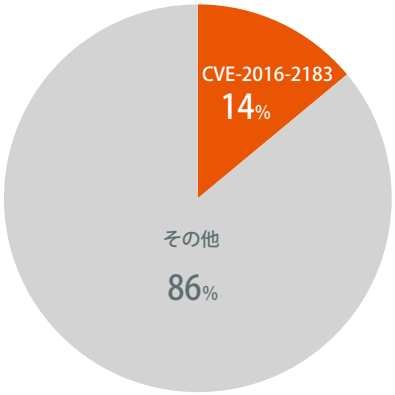
●終焉を迎える3DES

2019年3月、米国国立標準技術研究所(NIST※m)は2023年以降における3DES(3 Data Encryption Algorithm)の利用を不可とするガイドライン※nを公表しました。3DESは、共通鍵ブロック暗号の一つであるDESを暗号化、復号、暗号化の順に3回実行することで安全性を強化した暗号アルゴリズムのことで、長く利用されてきました。しかし、3DESには複数の脆弱性が存在しており、中でも影響範囲の広いのが、2016年に公表されたSweet32と呼ばれる脆弱性(CVE-2016-2183)です。Sweet32は暗号文を解読する際に、誕生日パラドックスと呼ばれる数学的な理論を用いることで、通常よりも高速に解読することができます。悪用された場合にはHTTPS通信のデータから暗号化されたデータの一部(例:Cookie)を解読される恐れがあります。

2018年のプラットフォーム診断では、検出した脆弱性のうちSweet32の検出が最多となりました(図19)。このことから、未だに3DESを有効にしているシステムが多いことがわかります。これは、サーバやソフトウェアの暗号設定を構築時から変更せずに運用していたためと考えられます。

対策はサーバ側でDESと3DESを無効化することです。設定変更の詳細については、独立行政法人情報処理推進機構(IPA※p)発行の「SSL/TLS暗号設定ガイドライン～安全なウェブサイトのために(暗号設定対策編)～※p」を参考にしてください。また、代替となる共通鍵ブロック暗号には、総務省および経済産業省が発行している「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)※q」で推奨されているものを利用する必要があります。

図19 2018年にSweet32が検出された割合



※m NIST:National Institute of Standards and Technologyの略。暗号化技術などの工業規格の標準化を行うアメリカ合衆国の政府機関
※n ガイドライン:「NIST SP 800-131A」https://www.nist.gov/publications/transitioning-use-cryptographic-algorithms-and-key-lengths
※o IPA:Information-technology Promotion Agency, Japanの略。IT施策を実施する経済産業省所管の機関
※p 独立行政法人情報処理推進機構(IPA「SSL/TLS暗号設定ガイドライン～安全なウェブサイトのために(暗号設定対策編)～」:https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
※q 電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト):https://www.cryptrec.go.jp/list.html

ラックの「セキュリティ診断」ラインナップ

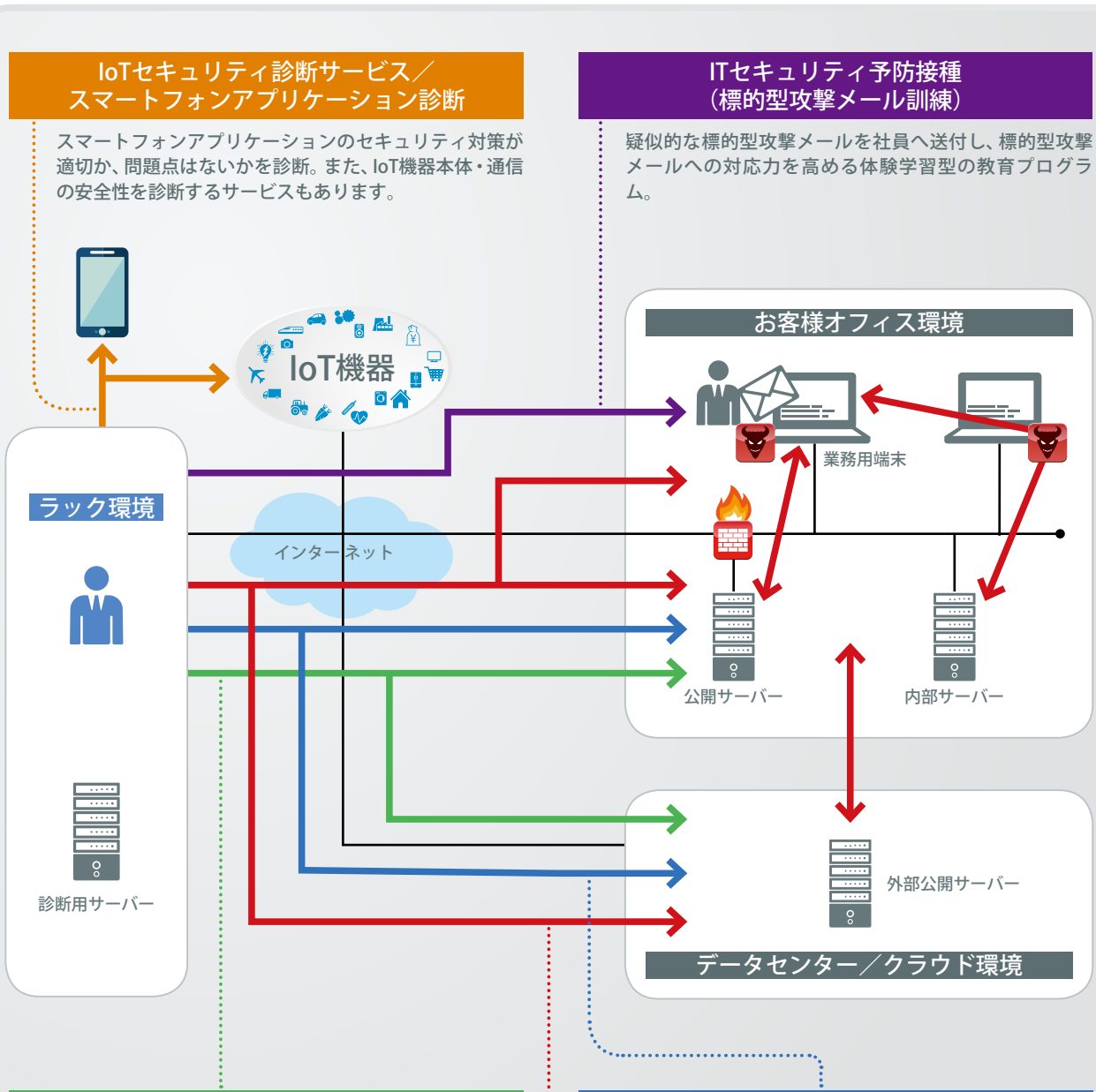
セキュリティ診断とは、お客様のITシステムに対して攻撃者の視点から考察した疑似攻撃を試行することで
リスクや脆弱性を見出し、対策を進めるためのサービスです。
ITシステムは多様な機器や製品、サービスを複雑に組み合わせて構築されています。
そのため、ラックではそれぞれの分野に細分化して、セキュリティ診断サービスを提供しています。

IoTセキュリティ診断サービス／スマートフォンアプリケーション診断

スマートフォンアプリケーションのセキュリティ対策が適切か、問題点はないかを診断。また、IoT機器本体・通信の安全性を診断するサービスもあります。

ITセキュリティ予防接種（標的型攻撃メール訓練）

疑似的な標的型攻撃メールを社員へ送付し、標的型攻撃メールへの対応力を高める体験学習型の教育プログラム。



プラットフォーム診断

サーバーやネットワーク機器に対して、不正アクセスの観点から侵入手法を考察・試行し、安全性を徹底的に調査します。ツールのみの低価格版も用意しています。

Webアプリケーション診断

攻撃者の視点からさまざまな疑似攻撃を考察・試行することで、ショッピングサイトや会員制サイトなど、Webアプリケーションの安全性を徹底的に調査します。

ペネトレーションテストサービス（侵入テスト）

お客様が運用しているITシステムに対して疑似攻撃を行います。成功した場合は、どこまで侵入でき、どのような情報を持ち出せるかを調査して、被害拡散リスクの評価を行います。

セキュリティ診断内製化支援サービス

お客様のセキュリティ診断の内製化を要所要所でバックアップし、運用の定着を手厚くサポートします。Webアプリケーション診断やプラットフォーム診断の両方に対応しています。

株式会社ラック セキュリティ診断センター
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
E-MAIL：sales@lac.co.jp　https://www.lac.co.jp